ASAF 4.6.2025 Helsinki

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

OT-vaikuttamisen trendit, havainnot ja saadut opit Ukraina-ikkunassa 2022-2025

Kimmo Saarni, Erityisasiantuntija
Liikenne- ja viestintävirasto,
Kyberturvallisuuskeskus

Traffic Light Protocol -käsittelyluokitus

TLP:RED - Vain vastaanottajalle

TLP:AMBER+STRICT - Vain vastaanottajan organisaatiolle "yksilöity tarve tietää" -periaatteella.

TLP:AMBER - Vain vastaanottajan organisaatiolle sekä organisaation asiakkaille "yksilöity tarve tietää" -periaatteella.

TLP:GREEN - Rajoitettu jakelu. Tieto voidaan jakaa vapaasti sen vastaanottajan edustaman organisaation sisällä, organisaation sidosryhmille, asiakkaille, sekä toimialalle/yhteisölle.

TLP:CLEAR - Tieto voidaan jakaa pakottavasta lainsäädännöstä johtuvat rajoitukset huomioiden vapaasti.

Lisätietoa tiedonvaihtokäytännöistä on ohjeessa https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

TLP:AMBER

Agenda

- Viranomaiset
- Yhteistyö
- Kybersää
- Teollisuuden ilmiöt
- Kyberturvallisuuskeskuksen palvelut
- Keskustelu

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Viranomaiskenttä ja kyberturvallisuuskeskus

Keskeiset tietoturva- ja kyberturvallisuusviranomaiset

POLIISI POLISEN I FINLAND Police of Finland	**Keskusrikospoliisi**	Poliisitoiminta, kyberrikollisuus
SUPO SUOJELUPOLIISI SKYDDSPOLISEN	**Suojelupoliisi**	Siviilitiedustelu, tilannekuva, attribuutio
Puolustusvoimat Försvarsmakten • The Finnish Defence Forces	**Puolustusvoimat**	Sotilastiedustelu, maanpuolustus kyberympäristössä
TRAFICOM Liikenne- ja viestintävirasto	**Liikenne- ja viestintävirasto Traficom**	Kyberturvallisuuskeskus, tilannekuva
DIGI- JA VÄESTÖTIETOVIRASTO	**Digi- ja västötietovirasto**	Digitalisaatio
TIETOSUOJAVALTUUTETUN TOIMISTO	**Tietosuojavaltuutetun toimisto**	Henkilötiedot, tietosuojaloukkaukset
VALTIOVARAINMINISTERIÖ FINANSMINISTERIET	**Valtiovarainministeriö**	Julkisen hallinnon ICT
Ulkoministeriö Utrikesministeriet	**Ulkoministeriö**	Kyberdiplomatia, kansallinen turvallisuusviranomainen, attribuutio
LIIKENNE- JA VIESTINTÄMINISTERIÖ KOMMUNIKATIONSMINISTERIET	**Liikenne- ja viestintäministeriö**	Kyberstrategia, sääntely (mm. NIS2)

Kansallinen kyberturvallisuuden tilannekuva

Suomalaisiin tietojärjestelmiin kohdistuvien tietoturvaloukkausten ja -uhkien selvittäminen

Tuki varautumisen, tieto-turvallisuuden sekä yksityisyyden suojan toteutumiseen viestintä-verkoissa ja sähköisessä viestinnässä.

Julkisesti säännellyn satelliittipalvelun (Galileo PRS) vastuuviranomainen

Tietojärjestelmien ja salaustuotteiden arviointi ja hyväksyntä sekä salausteknisen materiaalin jakelu

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen kansallinen koordinointikeskus

ohjaus
valvonta
tuotteet
palvelut
havainnointi
varoitukset
arvioinnit
rahoitus
osaaminen
verkostot

Traficomin Kyberturvallisuuskeskus on mukana rakentamassa maailman toimivinta ja turvallisinta digitaalista yhteiskuntaa

Perustettu **2014**

Budjetti **~26 M€**

Henkilöstö **190**

Verkosto-tapaamisia **~440**

Tarkastuksia **~40**

Julkaistuja tiedotteita **~150**

Automaattisesti käsiteltyjä tapahtumia **~200 000**

Käsiteltyjä tietoturvapoikkeamia **~19 000**

TRAFICOM

TLP:CLEAR

Kyberturvallisuuskeskus

Kyberturvallisuuskeskus tukee Suomen kriittistä infrastruktuuria havainnoimalla uhkia sekä ylläpitämällä luottamuksellisia tiedonjakoryhmiä ja kansallista kyberturvallisuuden tilannekuvaa.

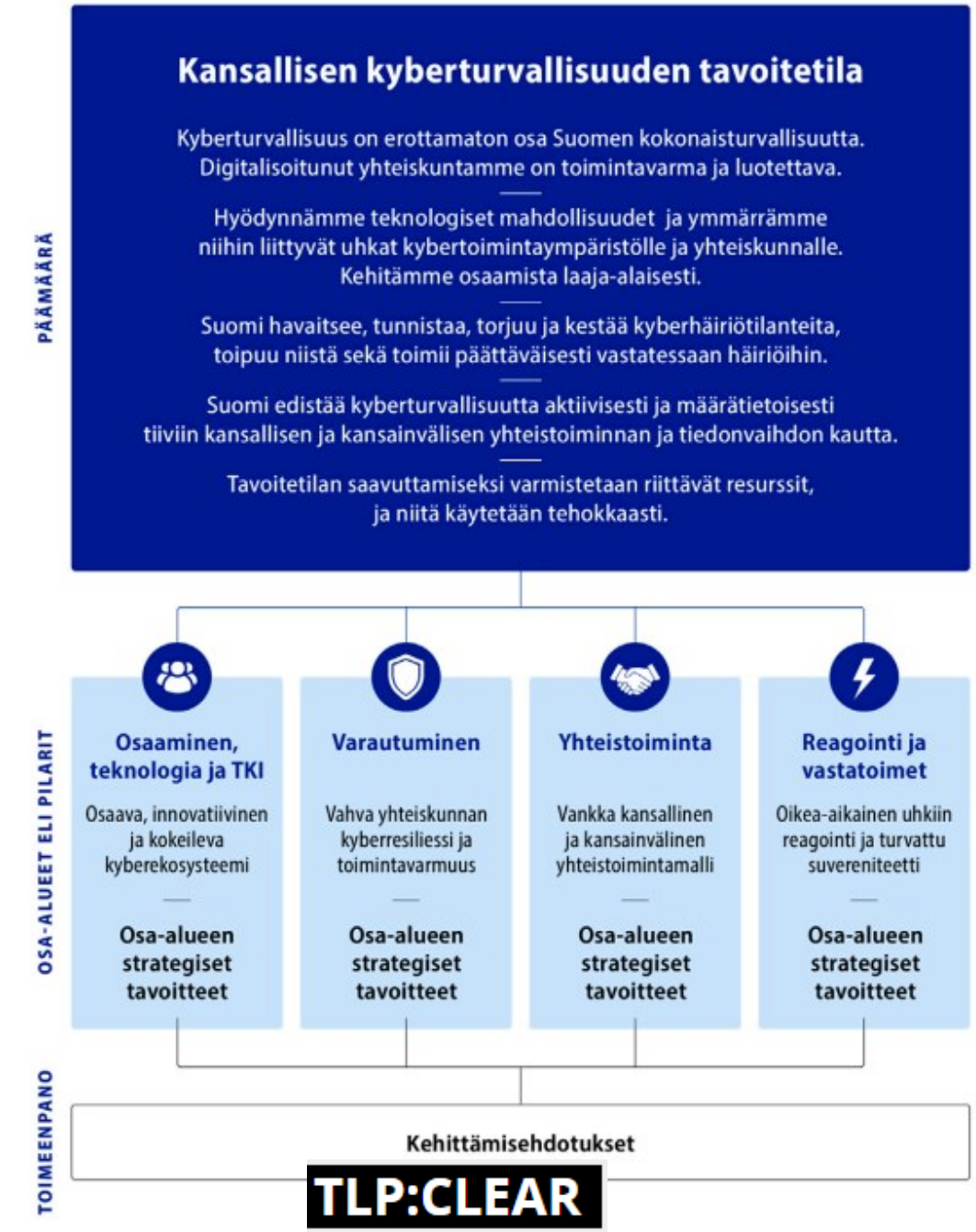
TLP:CLEAR

VALTIONEUVOSTON KANSLIAN JULKAISUJA 2024:11

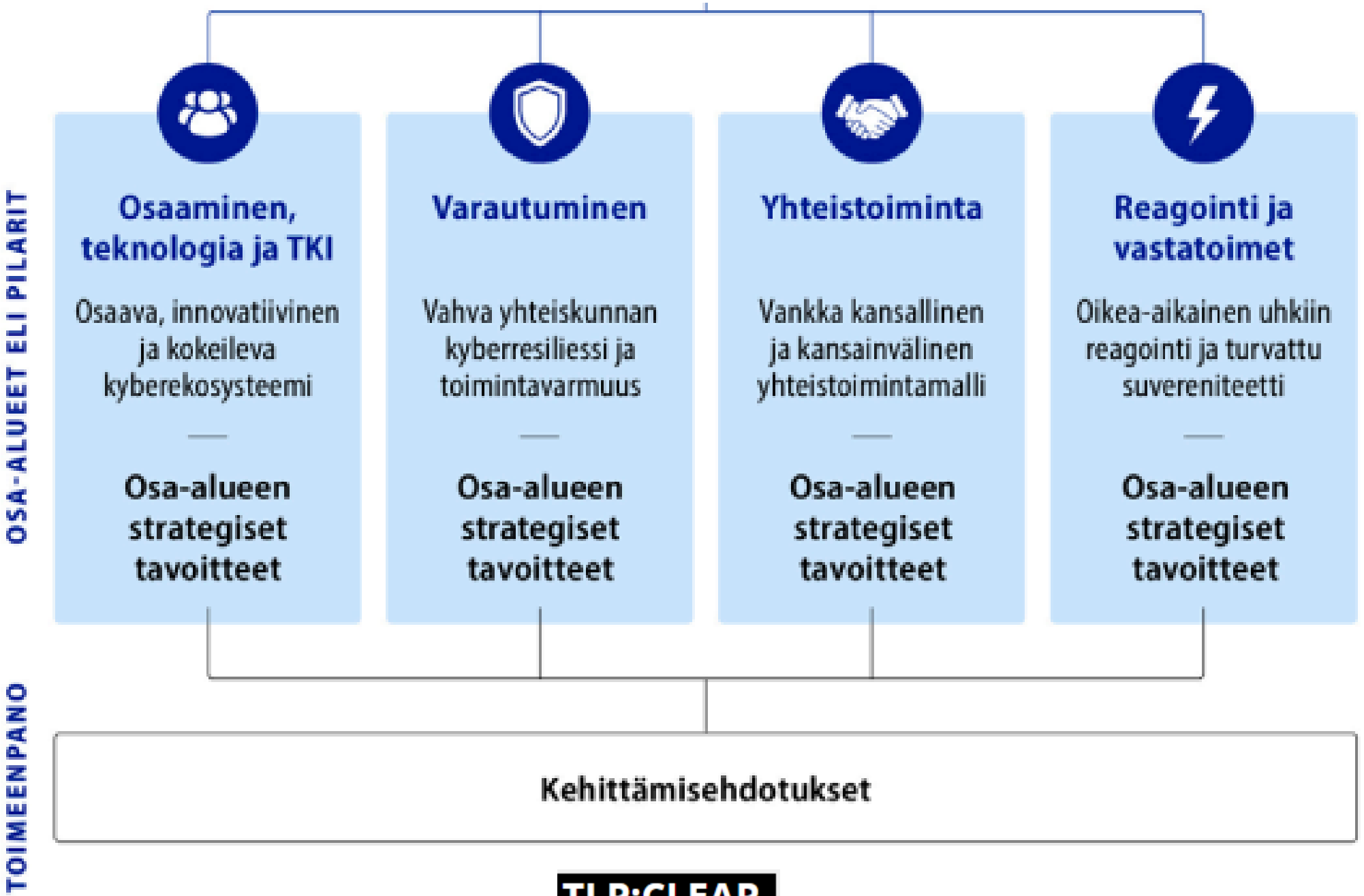
Suomen kyberturvallisuus-strategia 2024–2035

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

Kuva 1. Kyberturvallisuusstrategian tavoitetila ja strategian rakenne



Kuva 1. Kyberturvallisuusstrategian tavoitetila ja strategian rakenne


OSA-ALUEET ELI PILARIT
Osaaminen, teknologia ja TKI
Osaava, innovatiivinen ja kokeileva kyberekosysteemi
Osa-alueen strategiset tavoitteet
Varautuminen
Vahva yhteiskunnan kyberresiliessi ja toimintavarmuus
Osa-alueen strategiset tavoitteet
Yhteistoiminta
Vankka kansallinen ja kansainvälinen yhteistoimintamalli
Osa-alueen strategiset tavoitteet
Reagointi ja vastatoimet
Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti
Osa-alueen strategiset tavoitteet
TOIMEENPANO
Kehittämisehdotukset

TLP:CLEAR

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kybersää huhtikuu 2025

Tietomurrot ja -vuodot

- Huhtikuu oli tietomurtojen osalta alkuvuotta hiljaisempi.
- Hotelli- ja matkavarauspalveluiden murrettuja käyttäjätunnuksia erityisesti Booking.com-palvelussa käytettiin jälleen varauksen tehneiden asiakkaiden maksukorttitietojen kalasteluun.
- M365-tunnusten murrot jatkuivat ja erityisesti Dropbox-teemaiset AiTM-kalasteluviestit korostuivat.

Huijaukset ja kalastelut

- Aktiivista pankkitunnuskalastelua. SMS-huijausviestien teemoina on käytetty Tullia ja verottajaa, joiden nimissä on huijattu uhri klikkaamaan kalastelusivulle.
- Myös pysäköintivirhemaksulla pelottelemalla on ohjattu kalasteluun.
- Mobiilivarmenteen käyttäjiä on yritetty huijata hyväksymään tuntemattomia tunnistustapahtumia.

Haittaohjelmat ja haavoittuvuudet

- SAP NetWeaver -ohjelmistokomponentin kriittinen ja hyväksikäytetty haavoittuvuus (CVE-2025-31324) tulisi päivittää viipymättä.
- Ivanti Connect Secure -tuotteen kriittinen ja hyväksikäytetty haavoittuvuus (CVE-2025-22457). Vanhat versiot tulisi päivittää viipymättä.

Automaatio ja IoT

- Huhtikuu tarjosi hyvää kevätsäätä automaatio tai IoT –järjestelmien osalta, eikä tarkastelujaksolla tehty merkittäviä havaintoja.
- Yhdysvaltalaiset viranomaiset julkaisivat 6.5. ohjeen "Primary Mitigations to Reduce Unsophisticated Cyber Threats to Operational Technology".[14]

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäverkoissa havaittiin kuusi toimivuushäiriötä, joista yksi oli korkean vakavuusluokan häiriö (A).
- Alue- ja kuntavaaliviikolla venäjämielinen haktivistiryhmä kohdisti palvelunestohyökkäyksiä suomalaisille verkkosivuille, muun muassa puolueiden kotisivuille. Hyökkäyksillä ei ollut merkittäviä vaikutuksia vaalien sujumiseen.

Vakoilu

- Apple on lähettänyt varoituksia käyttäjilleen, joita on vakoiltu kaupallisilla vakoiluhaittaohjelmilla.
- Ranska yhdisti useat tutkimansa kyberhyökkäykset venäläiseen APT28-toimijaan.
- Puolassa ja Romaniassa paljastui valtionhallintoon ja yksityiseen sektoriin kohdistunutta vakoilua, jossa hyödynnettiin Microsoftin haavoittuvuutta.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Traficom julkaisi huhtikuussa uuden ohjeen tietojärjestelmien ja tietoturvallisuuden arviointi- ja hyväksyntäprosessista. Ohje on tarkoitettu viranomaisille ja yrityksille, jotka on käsitteleväät kansallista tai kansainvälistä turvallisuusluokiteltua tietoa sähköisesti.[4]

NIS 2 -direktiivin velvoitteet ja kyberturvallisuuslaki astuivat voimaan 8.4.2025. Uusi laki luo struktuuria Suomen kyberturvallisuudelle ja asettaa samalla yhteiskunnan kriittisille toimijoille velvollisuuksia kyberturvallisuuden poikkeamiin liittyen.[15]

Kevään aikana on havaittu useita haavoittuvuuksia etenkin verkon reunalaitteissa. Haavoittuvuuksien hallinta on haastavaa, mikäli organisaatio ei tunne ympäristöään riittävän kattavasti. Järjestelmien kartoitus ja dokumentointi on syytä tehdä säännöllisesti.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2.

Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.

3.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

Symbolit

- Uusi
- Päivitetty

4.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

5.

Tietoliikenneinfran suojaamisen tärkeys korostuu

Tietoliikenne- ja tietojärjestelmäinfran suojaaminen maailmalla ja kotimaassa on tärkeää, sekä siihen kohdistuvien vahinkojen ja luonnonilmiöiden että ulkopuolisten aiheuttamien tahallisten häiriöiden takia.

Teollisuuden ilmiöt 2022–2025

Kyberturvallisuus & vaikuttaminen

Yhteenveto

TLP:AMBER

Esityksen uhkatekijät pohjautuu havaintoihin aikaväliltä 2022 - 2025, jolloin geopoliittinen tilanne on kiristynyt merkittävästi. Emme siis tarkastele pelkästään Ukrainassa nähtyjä ilmiöitä.
Havainnot on kerätty julkisista raporteista sekä viranomaisyhteistyön ja kansallisten- ja kansainvälisten sidosryhmien kautta.

Esityksessä keskitytään kolmeen aiheeseen;

Haktivismi
-Hyökkäykset kohdistuvat heikosti suojattuihin järjestelmiin.
-Tavoitteena järjestelmien häirintä ja informaatiovaikuttaminen, esim. vuodoilla somessa.
-Kohdeorganisaatiot voivat joutua mediahuomion ja mainehaitan kohteeksi.

Sabotaasi
-Toiminnan lamauttaminen taloudellisista tai poliittisista syistä
-Tekijöinä voi olla ulkoinen taho, kilpailija tai sisäinen toimija
-Sabotaasin valmisteluun ja tiedon hankintaan käytetään mm. avoimia julkisia lähteitä
-Tavoitteena psykologinen ja taloudellinen vaikutus

Vakoilu
-Vakoiluoperaatiot ovat muuttuneet pitkäjänteisiksi ja ennakoiviksi
-Tietoa hankintaan avoimista lähteistä, tietojen kalastelulla tai lähestymällä henkilöstöä.
-Tavoitteena prosessien ymmärrys ja valmistautuminen laajempaan vaikuttamiseen.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tiedonvaihto ja yhteistyö

Verkostot tuottavat ja jakavat tietoa

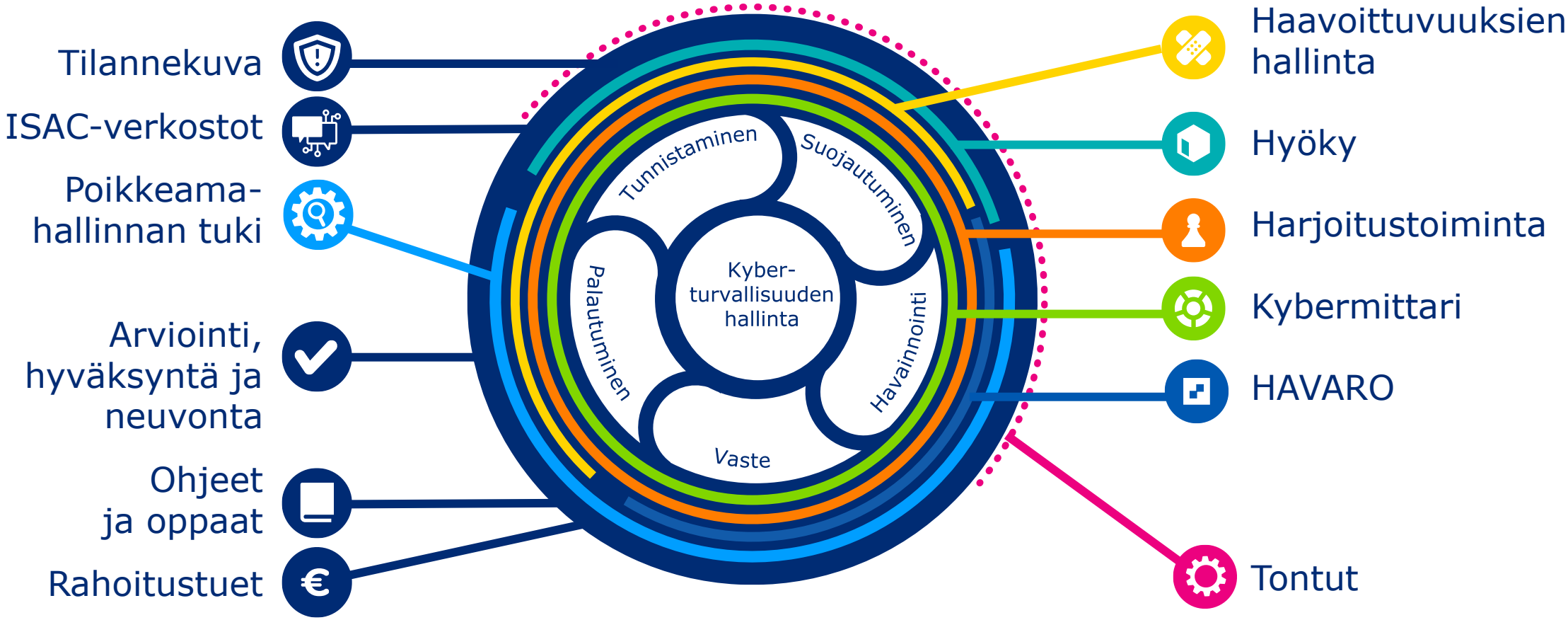
Kyberturvallisuuden kehittämistä, suunnittelua ja varautumista koordinoi **valtion kyberturvallisuusjohtajan toimisto**.

ISAC-verkosto (Information Sharing and Analysis Centres) koostuu noin 300 organisaatiota. ISAC-toiminta perustuu vapaaehtoisuuteen ja luottamukselliseen tiedonvaihtoon.

Kyberturvallisuus ei tunne valtioiden rajoja. Osallistumme aktiivisesti **avoimeen ja kansainväliseen tiedonvaihtoon** lukuisissa eri verkostoissa.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus keskuksen palvelut



Kyberturvallisuuskeskuksen palvelut kuuluvat kaikille

Palvelumme ovat pääsääntöisesti maksuttomia. Osa on suunnattu erityisesti tukemaan valtionhallinnon ja huoltovarmuuskriittisten organisaatioiden kyberturvallisuutta.

Keskustelua kysymyksiä kommentteja ?